UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,698	09/25/2003	Eduard K. de Jong	SUN-P7008	9219

24209 7590 05/30/2008

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,698	DE JONG, EDUARD K.	
	Examiner	Art Unit	
	DANIEL L. HOANG	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *See Continuation Sheet* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3 to 4, 8 to 10, 12, 14, 15, 19 to 21, 23, 25, 26, 30 to 32, 34, 36, 37, and 41 to 43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims pending in the application are 1, 3 to 4, 8 to 10, 12, 14, 15, 19 to 21, 23, 25, 26, 30 to 32, 34, 36, 37, and 41 to 43 .

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3 to 4, 8 to 9, 12, 14, 15, 19 to 20, 23, 25, 26, 30 to 31, 34, 36, 37, and 41 to 42, are rejected under 35 U.S.C. 103(a) as being unpatentable over Torrubia-Saez, US Patent No. 6,966,002, hereinafter Saez, and further in view of Levy, US Patent No. 6640279

As per claim 1, 12, 23, 34, Saez teaches:

A method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

Issuing, from a user device to an application program provider, an enrollment request comprising a target ID *["system identification information"]*, said enrollment request for receipt of one or more obfuscated application programs *["software product"]* controlled by said application program provider *["server"]*, said target ID specifying said user device *["components of the user's computer"]* configured to execute said one or more obfuscated application programs;

> *[see col. 18, lines 6-9] "the server sends a software product, which is either an executable object or a data object, to the user's computer, in response to a request sent to the server from the user's computer."*
>
> *[see col. 18] "In response to input from the user, an access control executable portion of the software product (if an executable object) or of the driver executable (if the software product is a data object) causes the user's computer to transmit a purchase request for partial or full access to the software product, and the server receives the purchase request. Step 1240 follows, at which the server sends to the user's computer a program which generates system identification information based on data that is specific to the user's computer. For example, the data used to generate the system identification information may include serial numbers of such components of*

> *the user's computer as the hard disk, the network interface card, the motherboard, and so forth. The user's computer then sends to the server the resulting system identification information, as well as information, such as a credit card number, which is required to complete the transaction. This information is received at the server, as indicated at step 1250. Following step 1250 is step 1260, at which the server validates the credit card information and generates a decryption key and/or a decryption executable program on the basis of the system identification information received from, and specific to, the user's computer.*"

obtaining, on said user device from said application program provider, a secret in response to said issuing; and

> [see col. 18, lines 49-51] "*The decryption key and/or decryption executable program are then transmitted to the user's computer from the server, as indicated at step 1270.*"

associating, on said user device, said secret with said application program provider, said secret for use in executing said one or more obfuscated application programs received from said application program provider.

> [see col. 18, lines 52-55] "*The decryption key and/or decryption executable program are then used in the user's computer to decrypt the software object to which the user has just purchased usage rights.*"

Saez does not explicitly teach:

The reception of said one or more obfuscated executable application programs occurs after obtaining a secret, which occurs in response to an enrollment request. In contrast, Saez teaches that the obfuscated executable application programs are received after the enrollment request is issued but before a secret is obtained. After further consideration, examiner determines that it would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Saez invention in order to allow the system taught by Saez to receive the program after the secret is obtained. Sending the program after the secret is obtained would allow the server to encrypt the program based on the requestor's secret. The requestor can then receive the encrypted program and decrypt it accordingly using its secret. Examiner deems these processes of encryption/decryption are well known in the art.

Saez also is mute in teaching that the user device comprises a smart card and said smart card comprises a virtual machine and said target ID comprises a VM ID. For this limitation, examiner relies upon the Levy reference. Please refer to fig 5 of the reference wherein Levy teaches a smart card comprising a virtual

machine. It would have been obvious to one of ordinary skill in the art to modify the system taught by Saez to have the device be a smart card because this allows the device to be small, low-cost, portable, and still security-sensitive. The above advantages would motivate one to implement the device taught by Saez in a smart card, as taught by Levy.

As per claim 3, 14, 25, 36, Saez teaches:

A method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

receiving an enrollment request comprising a target ID, said enrollment request for access by a user device to one or more obfuscated application programs, said target ID specifying said user device, said user device configured to execute said one or more obfuscated application programs;

[see rejection of claim 1]

determining a secret in response to said request; associating said secret with said target ID; and

[see rejection of claim 1, "the server validates the credit card information and generates a decryption key and/or a decryption executable program on the basis of the system identification information received from, and specific to, the user's computer."]

transferring said secret to said user device.

[see col. 18, lines 49-51] "The decryption key and/or decryption executable program are then transmitted to the user's computer from the server, as indicated at step 1270."

As cited above in claim 1, Saez is mute in teaching that the user device comprises a smart card and said smart card comprises a virtual machine and said target ID comprises a VM ID. For this limitation, examiner relies upon the Levy reference. Please refer to fig 5 of the reference wherein Levy teaches a smart card comprising a virtual machine. It would have been obvious to one of ordinary skill in the art to modify the system taught by Saez to have the device be a smart card because this allows the device to be small, low-cost, portable, and still security-sensitive. The above advantages would motivate one to implement the device taught by Saez in a smart card, as taught by Levy.

As per claim 4, 15, 26, 37, Saez teaches:

The method of claim 3 wherein said determining and said transferring form part of a key exchange protocol.

[see rejection of claim 3, wherein the generating and transmitting of the decryption key are considered as forming part of a key exchange protocol.]

As per claim 8, 19, 30, 41, Saez teaches:

A method for application program obfuscation, the method comprising:

determining a current obfuscation method based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

[see rejection of claim 1] "the server validates the credit card information and generates a decryption key and/or a decryption executable program on the basis of the system identification information received from, and specific to, the user's computer."

The decryption key that will be generated is based in part on the payment authorized by user's credit card as well as system identification information. Depending on the amount of payment, user will be authorized to use certain portions/versions of the software product. The appropriate decryption key will be generated allowing user access to said portions.

creating an obfuscated application program based at least in part on said current obfuscation method; and

[see col. 3] "a software package is provided, comprising: a software object having a first set of features and a second set of features, the first set of features being encrypted and the second set of features being unencrypted; and a signature readable by a predetermined executable serving to control access to the encrypted first set of features."

sending said obfuscated application program to said user device.

[see rejection of claim 1]

As cited above in claim 1, Saez is mute in teaching that the user device comprises a smart card and said smart card comprises a virtual machine and said target ID comprises a VM ID. For this limitation, examiner relies upon the Levy reference. Please refer to fig 5 of the reference wherein Levy teaches a smart card comprising a virtual machine. It would have been obvious to one of ordinary skill in the art to modify the system taught by Saez to have the device be a smart card because this allows the device to

be small, low-cost, portable, and still security-sensitive. The above advantages would motivate one to implement the device taught by Saez in a smart card, as taught by Levy.

As per claim 9, 20, 31, 42, Saez teaches:

The method of claim 8, further comprising receiving an application program request from said user device, said determining occurring in response to said receiving.

[see rejection of claim 1, wherein the decryption key is generated after the user requests the software product.]

Claims 10, 21, 32, 43, are rejected under 35 U.S.C. 103(a) as being unpatentable over Saez and Levy, as applied to claims 8-9 above, and further in view of Rusnak et al., US Patent No. 6,098,056.

As per claim 10, 21, 32, 43:

The method of claim 8 wherein said method further comprises, after said creating, applying a cryptographic process to said obfuscated application program together with a cryptographic key to create an encrypted obfuscated application program; and said sending comprises sending said encrypted obfuscated application program.

The Saez reference has been discussed above. Saez does not teach applying a cryptographic process to the obfuscated application program to create an encrypted obfuscated application program. Rusnak teaches doubly encrypting a document encryption key (DEK) as seen below:

[see col. 3] "After authentication, the server decrypts the DEK with its private key; encrypts the newly encrypted DEK with TIH's public key; encrypts the decrypted key with the client's public key; and returns the doubly encrypted DEK to the client."

It would have been obvious at the time of the invention to one of ordinary skill in the art to modify the Saez invention to doubly encrypt the content being transmitted in order to authorize and authenticate both user and server, thus improving the overall security of the system.

Conclusion

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2136

/Brandon S Hoffman/
Primary Examiner, Art Unit 2136